525 Rec'd PCT/PTO 20 DEC 2000

FORM PTO-1390 (REV 10-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: T2146-906752

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/720085

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR00/01047	April 20, 2000	April 20, 1999

TITLE OF INVENTION: SIGNATURE VERIFICATION AND AUTHENTICATION METHOD

APPLICANT(S) FOR DO/EO/US: Louis GOUBIN and Jacques PATARIN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)).
4. [X] The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto (required only if not communicated by the International Bureau).
   b. [X] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 16 below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. to CP8
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [X] A change of power of attorney and/or address letter.
16. [X] Other items or information:
    Verification of Translation
    Proposed Drawing Corrections
    PCT Documents-PCT/RO/101; PCT/IB/301, 304 & 308; Notif. of Nat'l Reg. No. Demand

JC01 Rec'd PCT/PTO 20 DEC 2000

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/720085	PCT/FR00/01047	T2146-906752

17. [X] The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**

	CALCULATIONS PTO USE ONLY	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	21 - 20 =	1	X **$18.00**	$ 18.00	
Independent claims	1 - 3 =	0	X **$80.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$	
TOTAL OF ABOVE CALCULATIONS =				$ 878.00	
[ ] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				$	
SUBTOTAL =				$ 878.00	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 878.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$918.00	
				Amount to be refunded:	$
				charged:	$

a. [X] A check in the amount of $ 918.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 501165. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Edward J. Kondracki
MILES & STOCKBRIDGE P.C.
1751 Pinnacle Drive, Suite 500
McLean, VA 22102-3833

SIGNATURE

Edward J. Kondracki
NAME

20,604
REGISTRATION NUMBER

December 20, 2000

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Louis GOUBIN et al.

International Application No.: PCT/FR00/01047

International Filing Date: 20 April 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: December 20, 2000

For: **SIGNATURE VERIFICATION AND AUTHENTICATION METHOD**

McLean, Virginia

PRELIMINARY AMENDMENT

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as indicated below:

IN THE TITLE:

Delete the title in its entirety and substitute the following new title:

--METHOD FOR VERIFYING A SIGNATURE OR AN AUTHENTICATION—.

IN THE SPECIFICATION:

After the title and before the first paragraph on page 1, insert the following heading at the left-hand margin:

--FIELD OF THE INVENTION--;

Page 1, line 7, insert the following heading at the left-hand margin:

--BACKGROUND OF THE INVENTION--;

Page 1, at line 16, before the paragraph beginning "The majority,...", insert the following heading at the left hand margin:

--DESCRIPTION OF RELATED ART--;

Page 2, at line 5, and before the paragraph beginning "The object of the ..." insert the following paragraph at the left-hand margin:

--SUMMARY OF THE INVENTION--;

Page 3, at line 1 and before the first paragraph, insert the following heading at the left hand margin:

--BRIEF DESCRIPTION OF THE DRAWINGS--;

Page 3, at line 13 and before the paragraph beginning "A more detailed...", insert the following heading at the left hand margin:

--DESCRIPTION OF THE PREFERRED EMBODIMENT(S)--;

Page 6, line 29, after "zero", insert –subtraction by m--", and before "substraction", delete "a" and substitute –one--;

Page 8, after line 19, insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

IN THE CLAIMS:

Please cancel claims 1 – 13 in their entirety and without prejudice and substitute the following new claims:

--14. A method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key and public-key cryptographic calculation process between a "*prover*" entity and a "*verifier*" entity, wherein the prover entity performs first cryptographic calculations with said private key to produce a signature calculation, or respectively an authentication value constituting a response value, and the verifier entity, based on said response value, performs second cryptographic calculations with said public key to perform said signature verification, or respectively said authentication, the first and second cryptographic calculations serving to implement the calculation of modulo-n or large-number multiplications, characterized in that for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n, and a private key comprising a private exponent, it comprises the following steps"

- calculating at the level of said prover entity at least one prevalidation value;

- transmitting from the prover entity to the verifier entity at least said one prevalidation value, and utilizing said prevalidation value by the verifier entity to perform at least one modular reduction without any division operation for said modular reduction.

15. A method according to claim 14, characterized in that for a public exponent e=2, and wherein the cryptographic calculation process is based on a RABIN algorithm, said at least one prevalidation value comprises a unique value, which is the quotient Q of the square of said respective value of a signature or a response by said public modulo n, Q = R*R/n, where R designates said respective value of a signature or a response to an authentication.

16. A method according to claim 15, characterized in that after the reception by said entity of said respective value of a response to an authentication verification or a signature of a message (M), and of said at least

one prevalidation value comprising said quotient, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{AR}, D_{SR}) between the square of the response value R*R and the product Q*n of said quotient Q by said public modulo n, (D_{AR}, D_{SR} = R*R =Q*n; and
- verifying the equality of said difference with the value of a function of said response value, without any division operation by the modulo n operation.

17. A method according to claim 14, characterized in that for a public exponent e = 3, and wherein the cryptographic calculation process is based on an RSA algorithm, said at least one prevalidation value comprises:

- a first quotient Q_1 of the square R*R of said response value R by said public modulo n; and
- a second quotient Q_2 of the product of said response value and the difference between the square R*R of said response value and the product of said first quotient Q_1 and the public modulo n, by said public modulo n, Q_2 = $R*(R*R - Q_1*n)/n$.

18. A method according to claim 17, characterized in that after the reception of said response value R and said at least one prevalidation value comprising said first and second quotients Q_1 and Q_2, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{ARSA}, D_{SRSA}) between the product of said response value R and the difference between the square R*R of this response value and the product of said first quotient Q_1 and the public modulo n, and the product of said second quotient Q_2 and said public modulo n (D_{ARSA}, D_{SRSA}) = $R*(R*R - Q_1*n)-Q_2*n$; and
- verifying the equality of this difference with the value of a function of said response value, without any division operation by modulo n operation.

19. A method according to claim 16, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of said message M, said method comprises the following steps:

- applying a condensation function to said message to obtain a message digest CM; and
- concatenating said message digest with a constant value.

20. A method according to claim 18, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of said message M, said method comprises the following steps:

- applying a condensation function to said message to obtain a message digest CM; and
- concatenating said message digest with a constant value.

21. A method according to claim 16, characterized in that, for an authentication verification operation, said method further comprises the step for transmitting a prompt value from the verifier entity to the prover entity.

22. A method according to claim 18, characterized in that, for an authentication verification operation, said method further comprises the step for transmitting a prompt value from the verifier entity to the prover entity.

23. A method according to claim 21, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

24. A method according to claim 22, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

25. A method according to claim 16, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

26. A method according to claim 21, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

27. A method according to claim 22, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

28. A method according to claim 25, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

29. A method according to claim 26, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the

calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

30. A method according to claim 27, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A-n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of -C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction.

31. A method according to claim 23, characterized in that said function f(A) of said random value A is the function f(A) = A, which makes it possible to verify the equality of said difference and the validity of said authentication without any division operation for the modular reduction.

32. A method according to claim 24, characterized in that said function f(A) of said random value A is the function f(A) = A, which makes it possible to verify the equality of said difference and the validity of said authentication without any division operation for the modular reduction.

33. A method according to claim 14, characterized in that said response value, an encrypted value B, and a quotient value Q are concatenated prior to transmission of the values from the prover entity to the verifier entity.

34. A method according to claim 14, wherein the verifier entity compression embedded system such as a microprocessor card and the prover entity comprises an embedded card reading system.--

IN THE ABSTRACT:

Please cancel the Abstract at page 13 and substitute the following Abstract.

--ABSTRACT

The invention concerns a method for verifying a signature or an authentication between a prover and a verifier based on an asymmetric cryptographic calculation algorithm. The prover calculates (1) at least one prevalidation value q, which is a quotient of two cryptographic values a, b by the public modulo n, and transmits this value q to the verifier. The verifier calculates (3) the products a*b and q*n and the difference a*b-q*n in order to perform at least one modular reduction without a division operation. The invention applies to signature or authentication verification between a proving microcomputer and a verifying microprocessor card.--

REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice, to eliminate the use of multiple dependent claims, and to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text.

Early action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: December 20, 2000

By: Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

T2146-906752-US 3797/BC(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Louis GOUBIN et al.

International Application No.: PCT/FR00/01047

International Filing Date: 20 April 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: December 20, 2000

For: **SIGNATURE VERIFICATION AND AUTHENTICATION METHOD**

McLean, Virginia

PROPOSED DRAWING CORRECTIONS

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant requests approval of the drawing corrections on Figs. 1 – 3B as shown in red on the attached three (3) sheets.

The proposed corrections only comprise translating the French terms into English and removing the headings "1/3" – "3/3" to conform the drawings to U.S. practice.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: December 20, 2000

By: _____
Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

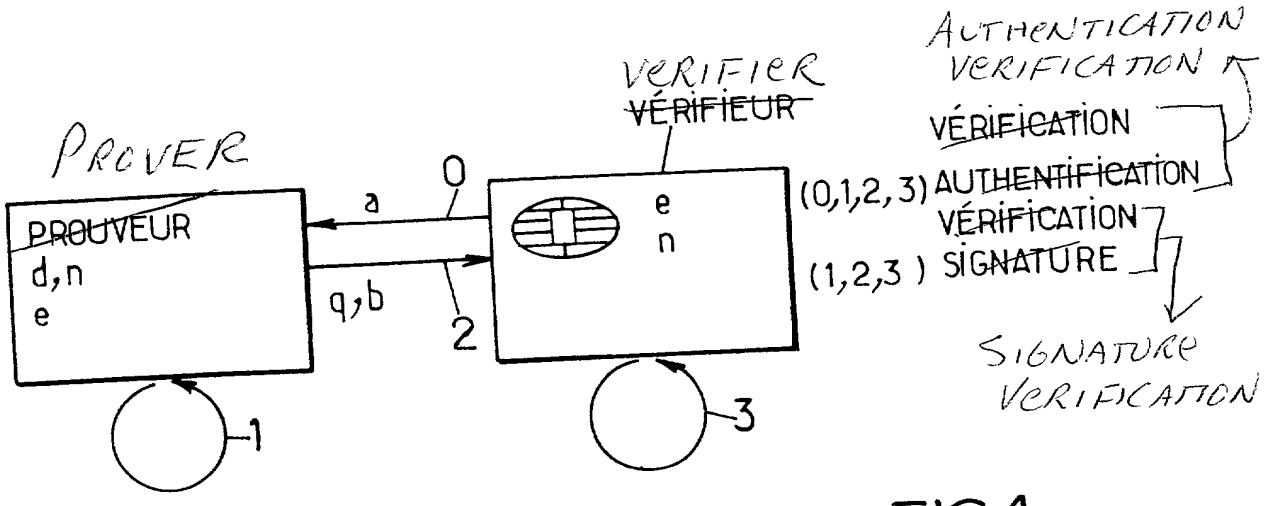


FIG.1.

$q = a * b / n$

$b = \begin{cases} a^d \bmod n & \text{si (0,1,2,3)} \\ S = Sd(M) & \text{si (1,2,3)} \end{cases}$

if

if

$a * b$

$q * n$

$a * b - q * n$

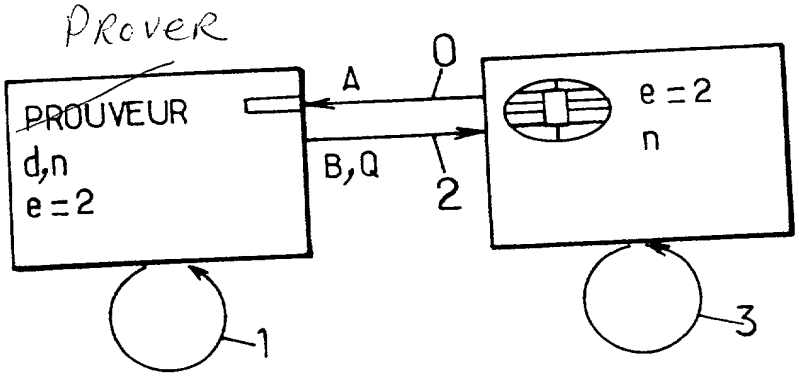


FIG. 2a.

$R = B = A^d \bmod n$

$Q = B * B / n$

$D_{AR} = B * B - Q * n$

$D_{AR} = A$

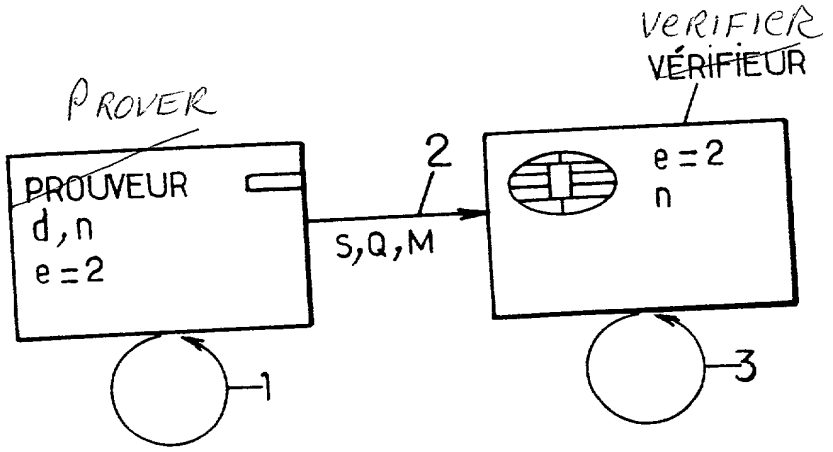
$D_{AR} = n - A$

$D_{AR} = C * A \bmod n = C * A$ si $C * A < n$

$D_{AR} = -C * A \bmod n = C * A - n$ SINON

IF

IF NOT



VÉRIFICATION
SIGNATURE SIGNATURE
VERIFICATION

$R = S = Sd(M)$

$Q = S * S / n$

$D_{SR} = S * S - Q * n$

$D_{SR} = f(M)$

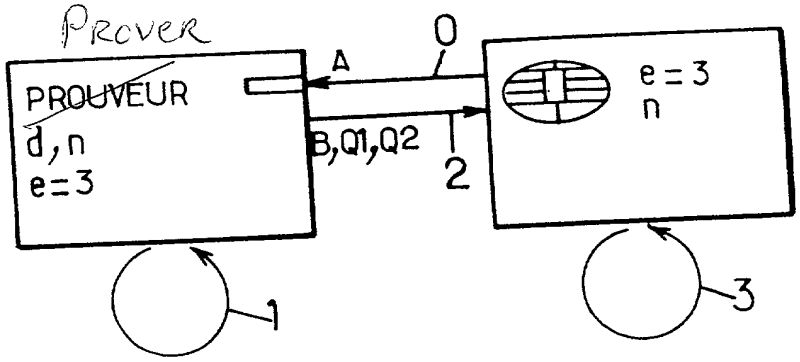
$= n - f(M)$

$= C * f(M) \bmod n = C * f(M)$ si $< n$

$= C * f(M) \bmod n = C * f(M)$ SINON

IF NOT

FIG.2b.



VÉRIFICATION
D'AUTHENTIFICATION
AUTHENTICATION
VERIFICATION

$R = B = A^d \bmod n$

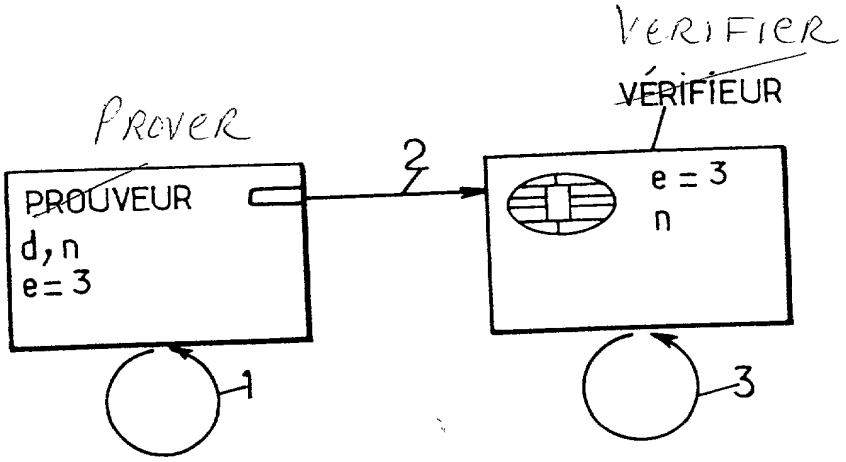
$Q1 = B * B / n$

$Q2 = B(B * B - Q1 * n) / n$

$D_{ARSA} = B(B * B - Q1 * n) - Q2 * n$

$D_{ARSA} = f(A) = A$

FIG.3a.



$R = S = Sd(M)$

$Q1 = S * S / n$

$Q2 = S(S * S - Q1 * n)/n$

$D_{SRSA} = S(S * S - Q1 * n) - Q2 * n$

$D_{SRSA} = f(M)$.

FIG.3b.

SIGNATURE VERIFICATION AND AUTHENTICATION METHOD

The present invention relates to a method that makes it possible to increase the efficiency, in terms of the calculation time and the RAM and ROM required, of the verification of a signature or an asymmetric authentication requiring several modulo-n or large-number multiplications.

The RSA and Rabin signature or authentication algorithms are examples that allow the implementation of this method.

The method is more particularly adapted to an implementation in the case of a computer, for example a personal computer designated PC, that generates a signature or an authentication by means of a secret key, which must then be verified by a microcomputer card. The microcomputer performs this verification by means of a public key. It has relatively little power compared to the PC.

The term "*microcomputer card*" is intended to mean a standard monolithic microcontroller with an incorporated memory.

The majority of public key algorithms used in the world today perform "*large-number*" modulo calculations. "*Large-number*" designates positive whole numbers of at least 320 bits. For security reasons, the scientific community currently recommends the use of numbers of at least 512 bits, or even 1024 bits for most of the algorithms, for example for the RSA or Rabin algorithms.

Currently, microcomputer cards are brought to dialog with computers having computing capacities much larger than their own. Moreover, for cost reasons, microcomputer cards without an arithmetic coprocessor and with very limited memory resources (ROM, RAM, EEPROM) are used. For this reason, the calculations normally required to perform an authentication verification or a public-key signature verification using large-number modulo calculations are often very long, or even impossible without enough memory, if the traditional descriptions of the cryptographic algorithms are used.

In the description below, the following terms mean:

- "*prover*": the entity that wishes to be authenticated, or that produces a signature. To do this, it performs calculations involving the secret key of the asymmetric algorithm used. It could be, for example, a computer of the PC type.

- *"verifier"*: the entity that verifies the authentication, or that verifies the validity of a signature. To do this, it performs calculations involving only the public key of the asymmetric cryptographic algorithm used. It can be, for example, a microcomputer card.

The object of the present invention is to implement a method for verifying signatures and authentications that makes it possible to eliminate the aforementioned disadvantages inherent in the more limited computing capacity of a verifying entity constituted by a microcomputer card, as compared to a proving entity such as a personal computer or the like equipped with a card reading device.

Consequently, another object of the present invention is to simplify the verifier's operations for calculating certain modular reductions through the implementation of additional calculations by the prover, the verifier's task thus being simplified without any reduction in the theoretical security of the system.

The method for verifying a signature, or respectively an authentication, by means of an asymmetric private-key and public-key cryptographic calculation process, which is the subject of the present invention, this method being implemented between a *"prover"* entity and a *"verifier"* entity, the prover entity performing cryptographic calculations with the private key in order to produce a signature calculation, or respectively an authentication value, and the verifier entity, based on this transmitted value, performing cryptographic calculations with this public key in order to perform this signature verification, or respectively this authentication, the cryptographic calculation operations implementing the calculation of modulo n or large-number multiplications, is remarkable in that for a cryptographic calculation process using a public key constituted by a public exponent e and a public modulo n, and a private key constituted by a private exponent d, this method consists of calculating, at the level of the prover entity, at least one prevalidation value and transmitting from the prover entity to the verifier entity this at least one prevalidation value, thereby allowing the verifier entity to perform at least one modular reduction without any division operation for this modular reduction.

The method that is the subject of the present invention applies to any dialogue or protocol for exchanging messages between a prover entity such as a personal computer and a verifier entity such as a microcomputer card, particularly in connection with banking transactions, access control, or the like.

It will be more clearly understood by reading the description below and examining the drawings, in which:

- Fig. 1 represents a diagram illustrating the method that is the subject of the present invention, implemented between a prover entity and a verifier entity;

- Fig. 2a represents a diagram illustrating the method that is the subject of the present invention, implemented with a Rabin authentication verification algorithm;

- Fig. 2b represents a diagram illustrating the method that is the subject of the present invention, implemented with a Rabin signature verification algorithm;

- Fig. 3a represents a diagram illustrating the method that is the subject of the present invention, implemented with an RSA authentication verification algorithm;

- Fig. 3b represents a diagram illustrating the method that is the subject of the present invention, implemented with an RSA signature verification algorithm.

A more detailed description of the method that is the subject of the invention is given in connection with Fig 1 and the subsequent figures.

The method that is the subject of the invention implements, at the verifier entity level, public-key algorithms requiring modulo-n or large-number multiplications, and modifies them slightly by having one or more quotients q calculated externally, i.e. at the prover entity level, and by supplying this quotient or quotients to the verifier. Thus, the verifier can more easily and quickly calculate certain modular multiplications: instead of calculating a*b modulo n, it only has to calculate a*b, q*n, and a*b-q*n, a and b designating values of the signature or authentication verification calculation. Sometimes, for security reasons,, it uses the latter value in a way that allows it to make sure that this latter value is actually between 1 and n. When an algorithm is thus modified by "*precalculating*" certain quotients that are supplied to the verifier in order to simplify the calculations executed by the latter, it is called a "*subjacent*" algorithm in order to designate the initial algorithm from which it is derived, prior to performing this modification. Thus, in reference to Fig. 1, according to a remarkable aspect of the method that is the subject of the present invention, the quotient or quotients q that verify the relation q=a*b/n constitute one or more prevalidation values transmitted to the verifier entity in order to allow the verifier entity to perform at least one modular reduction without any division operation for this modular reduction. Referring to Fig. 1, it is indicated that the method that is the subject of the invention can be implemented either when verifying the authentication after the sending of an

prompt value such as a random value a (see the reference 0 in the figure), the internal calculation (reference 1) at the prover level of a response value $b = a^d \bmod n$ and the prevalidation value q, the transmission (reference 2) of b and q from the prover to the verifier, and the calculation (reference 3) by the verifier of the quantities a*b, q*n and a*b-q*n in order to perform the verification of the authentication, or when verifying the signature of a message M after the calculation (reference 1) at the prover level of a signature $S = S_d(M)$ for the message M and the prevalidation value q, the sending (reference 2) of q, S and M from the verifier to the prover, the calculation (reference 3) at the verifier level of the quantities a*b = S*S, q*n and a*b-q*n in order to perform the signature verification.

In Fig. 1 and the subsequent figures, a straight arrow represents the transmission of the aforementioned values from the verifier to the prover or vice versa, and a looped arrow at the prover level or the verifier level represents the implementation of an internal calculation at the prover level or the verifier level. Finally, in the description below, the response R designates either the value b calculated by encrypting the random number a in the case of an authentication verification $b = a^d \bmod n$, or the signature value $S = S_d(M)$ following the connection of the verifier and the prover.

Various examples of the implementation of the method that is the subject of the present invention will now be described based on subjacent algorithms, designated by RSA and Rabin algorithms.

Subjacent RSA and Rabin algorithms

The RSA algorithm is the most famous of the asymmetric cryptographic algorithms. It was invented by RIVEST, SHAMIR and ADLEMAN in 1978. Its description may be found in:

R. L. Rivest, A. Shamir, L.M. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 21, No. 2, 1978, pp. 120-126, or in the following documents:

- ISO/IEC 9594-8/ITU-T X.509, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework;
- ANSI X9/31-1, American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry, 1993.

These documents are introduced into the present description as references.

The RSA algorithm uses a whole number n that is the product of two large prime numbers p and r, and a whole prime number e with ppcm(p-1, r-1), and such that e • $\pm$ 1 modulo ppcm(p-1 ,r-1). The integers n and e constitute the public key. The public key calculation uses the function α of $\mathbf{Z}/n\mathbf{Z}$ in $\mathbf{Z}/n\mathbf{Z}$ defined by $\alpha(x)=X^e \bmod n$. The secret key calculation uses the function $\alpha^{-1}(y)=y^d \bmod n$, where d is the secret exponent, also called the "*secret key*" or "*private key*," defined by $ed \equiv 1 \bmod ppcm(p-1, r-1)$.

Let n be the RSA public modulo, let d be the RSA secret exponent and let e be the RSA public exponent.

In the case of an authentication verification, the verifier generates a random number A modulo n, and sends it to the prover. The latter then calculates $B= A^d$ modulo n, and returns this value B to the verifier. The latter accepts the authentication if and only if B^e modulo n = A.

The smallest value of e for using the RSA algorithm is e = 3. For e = 2, the Rabin algorithm is used; the latter will be described later in the description. This value e = 3 is advantageous since it allows the verifier to have only two modular multiplications to perform.

The Rabin algorithm is similar to an RSA algorithm with the public exponent e = 2. In fact, when e = 2, the function x^e is not bijective modulo n, when n is the product of two prime numbers > 2, so slight modifications are introduced in the use of the Rabin algorithm as compared to the RSA algorithm.

A description of the Rabin algorithm may be found in:

M.O. Rabin, "Digitized Signatures and Public-Key Functions as Intractable as Factorization," Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979, introduced in the present patent application as a reference.

Exemplary implementations of the method that is the subject of the invention using the Rabin and RSA algorithms

♦ Rabin algorithm

The method that is the subject of the present invention will first be described in a particular non-limiting embodiment based on the Rabin algorithm, or for e = 2.

♦♦ Authentication verification

As represented in Fig. 2a, a possible example of the utilization of the Rabin algorithm in authentication verification is described below.

Let n be the public modulo. The verifier generates a random number A modulo n, and sends it (reference 0 in the figure) to the prover. The latter then calculates a number B (reference 1), and sends this value B to the verifier. The latter accepts the authentication if and only if B*B modulo n is equal to one of the following four possible values: A, or n-A, or C*A modulo n, or – C*A modulo n. C is a number set by the protocol, most often C = 2.

In order to simplify the verification process in accordance with the method that is the subject of the present invention, the prover does not send (reference 2) the value B alone: it sends B and Q, where Q is the quotient of B*B by the public modulo n. The verifier then verifies that D_{AR} = B*B = Q*n is actually equal to one of the following four values: A, n-A, (C*A) modulo n, or (-C*A) modulo n. In addition, it can calculate (C*A) modulo n, by calculating C*A, keeping this value if it is < n, and otherwise taking the value C*A – n. Thus, the verifier does not have any division to perform.

♦♦ Signature verification

Thus, as represented in Fig. 2b, and keeping the same notations as above, let M be the message whose signature S the verifier wishes to verify. The signature S is obtained from the private key d by S = S_d(M), S_d(M) designating the operation for calculating the signature of the message M. If S is a Rabin signature of M, then the verifier normally verifies that S*S modulo n = f(M) or n-f(M), or (2*f(M) modulo n) or (-2*f(M) modulo n), where f is a standardized public function of the message M. For example, f is the identity function, or is described in a signature standard; for example, it is possible o use the *padding* or concatenation operations of the PKCS#1 standard normally established for RSA; see the descriptive elements of this standard later in the description.

Keeping the same notations as above, in order to simplify the signature verification process as represented in Fig. 2b, in the method that is the subject of the present invention, the prover does not send (reference 2) the value S alone: it sends S and Q, where Q is the quotient of S*S by the public modulo n. The verifier then verifies that D_{SR} = S*S - Q*n is actually equal to f(M), or n-f(M), or C*f(M) modulo n, or –C*f(M) modulo n, where C is a number set by the protocol, C being able to be taken as equal to 2. Since these last two values can be modulo-n calculated by performing zero or a subtraction by n, the verifier no longer has any division to calculate.

♦ RSA algorithm

The method that is the subject of the present invention will now be described in a particular non-limiting embodiment based on the RSA algorithm, or for e = 3.

♦♦ Authentication verification

As represented in Fig. 3a, beginning with a random number A, in order to simplify the verification process, in the present invention, the prover does not send (reference 2) the value B alone: it sends B, Q1 and Q2, where Q1 is the quotient of B*B by the public modulo n, and where Q2 is the quotient of B* (B*B – Q1*n) by n. The verifier then verifies that D_{ARSA} = B*(B*B – Q1*n) –Q2*n is actually equal to A. Thus, the verifier no longer has any division to perform.

♦♦ Signature verification

Keeping the same notations as above and letting M be the message whose signature S the verifier wishes to verify, S is an RSA signature of M, so the verifier normally verifies that S^e modulo n = f(M), where f is a standardized public function of the message M. For example, f is the identity function, or is described in an RSA signature standard, such as for example the PKCS#1 standard. The standardized public function can consist of applying a condensation function SHA-1 to the message M in order to obtain a message digest CM, then of concatenating this message digest with a constant value.

Thus, as represented in Fig. 3b, and keeping the same notations as above, in order to simplify the signature verification process, in the method that is the subject of the present invention, the prover does not send (reference 2) the value S alone: it sends S, Q1 and Q2, where Q1 is the quotient of S*S by the public modulo n, and where Q2 is the quotient of S*(S*S – Q1*n) by n. The verifier then verifies that D_{SRSA} = S*(S*S = Q1*n) –Q2n is actually equal to f(M). Thus, the verifier no longer has any division to perform.

The condensation function SHA-1 is a public "*condensation*" function. It takes as input a message whose size can run from 0 bytes to several gigabytes, and yields as output a 160-bit "*digest*" of the message. This function is often used in standards or with signature algorithms, since it is reputed to be collision-resistant, which means that it is not known how to concretely find two separate messages that have the same message digest (they exist, but it is not known how to find such a pair of messages). This makes it possible to sign the message digests rather than the messages themselves.

The PKCS#1 standard is an RSA signature standard. It describes a public function f. This function f is applied to the message M to be signed with RSA before launching the RSA modular exponentiation operation itself: the RSA signature of M is therefore $S = (f(M))^d$ modulo n, where is the RSA public modulo and where D is the RSA secret exponent. f uses a condensation function (for example SHA-1) followed by a *padding*, or concatenation, with a constant.

For a more detailed conscription, please consult:

PKCS#1, *RSA Encryption Standard*, Version 2, 1998, available at the following address:

ftp://ftp.rsa/com/pub/pkcs/doc/pkcs-1v2.doc

whose published version is introduced in the present application as a reference.

The invention thus consists of supplying additional data to the verifier in order to facilitate its calculations. In order to precalculate this data, in this case the quotients constituting the prevalidation value or values, it is not necessary to use the secret key of the algorithm. This means that this data is completely redundant relative to the values transmitted to the card in a "*conventional*" utilization of the asymmetric algorithm. In fact, in the "conventional" version, the card knows how to find these quotients itself. There is therefore no additional information supplied to the card, in the sense of information theory, when the method that is the subject of the present invention is implemented as described above. This shows that the security of the system is in no way weakened as compared to the "*conventional*" implementation of the algorithm.

CLAIMS

1. Method for verifying a signature, or respectively an authentication, by means of an asymmetric private-key and public-key cryptographic calculation process between a "*prover*" entity and a "*verifier*" entity, the prover entity performing cryptographic calculations with said private key in order to produce a signature calculation, or respectively an authentication value constituting a response value, and the verifier entity, based on this response value, performing cryptographic calculations with said public key in order to perform this signature verification, or respectively this authentication, the cryptographic calculation operations implementing the calculation of the modulo-n or large-number multiplications, characterized in that for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n, and a private key comprising a private exponent, it comprises the following steps"

- calculating at the level of said prover entity at least one prevalidation value;
- transmitting from the prover entity to the verifier entity at least said one prevalidation value, this prevalidation value allowing the verifier entity to perform at least one modular reduction without any division operation for this modular reduction.

2. Method according to claim 1, characterized in that for a public exponent e=2, the cryptographic calculation processing being based on a RABIN algorithm, said at least one prevalidation value comprises a unique value, which is the quotient Q of the square of said respective value of a signature or a response by said public modulo n, Q = R*R/n, where R designates said respective value of a signature or a response to an authentication.

3. Method according to claim 2, characterized in that after the reception by said entity of said respective value of a response to an authentication verification or a signature of a message (M), and of said at least one prevalidation value comprising said quotient, this method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{AR}, D_{SR}) between the square of the response value R*R and the product Q*n of said quotient Q by said public modulo n, (D_{AR}, D_{SR} = R*R =Q*n;

- verifying the equality of said difference with the value of a function of this response value, without any division operation by the modulo n operation.

4. Method according to claim 1, characterized in that for a public exponent e = 3, the cryptographic calculation process being based on an RSA algorithm, said at least one prevalidation value comprises:

- a first quotient Q_1 of the square R*R of said response value R by said public modulo n;

- a second quotient Q_2 of the product of said response value and the difference between the square R*R of this response value and the product of said first quotient Q_1 and the public modulo n, by said public modulo n, $Q_2 = R*(R*R - Q_1*n)/n$.

5. Method according to claim 4, characterized in that after the reception of said response value R and said at least one prevalidation value comprising said first and second quotients Q_1 and Q_2, said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference (D_{ARSA}, D_{SRSA}) between the product of said response value R and the difference between the square R*R of this response value and the product of said first quotient Q_1 and the public modulo n, and the product of said second quotient Q_2 and said public modulo n (D_{ARSA}, D_{SRSA}) = $R*(R*R - Q_1*n)-Q_2*n$;

- verifying the equality of this difference with the value of a function of said response value, without any division operation by modulo n operation.

6. Method according to claim 3 or 5, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function f(M) of this message M, it comprises the following steps:

- applying a condensation function to this message in order to obtain a message digest CM;

- concatenating this message digest with a constant value.

7. Method according to either claim 3 or 5, characterized in that, for an authentication verification operation, this method also comprises the step for transmitting an prompt value from the verifier entity to the prover entity.

8. Method according to claim 7, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value A.

9. Method according to either of claims 3 and 7, characterized in that said function f(A) of said random value A comprises a function among the functions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

10. Method according to claim 9, characterized in that at the level of the verifier entity, the calculation of said function f(A) = C*A modulo n comprises the calculation of the value C*A and the storing of this value if $C*A < n$, and the calculation and storing of the value C*A-n if not, and in that the calculation of said function f(A) = -C*A modulo n comprises the calculation of the value n-C*A and the storing of this value if $n-C*A \geq 0$, and otherwise the calculation of the intermediate value C*n-C*A, and if this intermediate value is greater than or equal to zero, the calculation and storing of the value of -C*A modulo n, which makes it possible to verify the equality of said authentication without any division for the modular reduction.

11. Method according to claims 5 and 8, characterized in that said function f(A) of said random value A is the function f(A) = A, which makes it possible to verify

the equality of said difference and the validity of said authentication without any division operation for the modular reduction.

12. Method according to claim 1, characterized in that said response value, the encrypted value B, and said quotient value Q are concatenated prior to their transmission from the prover entity to the verifier entity.

13. Utilization of the method according to claim 1, the verifier entity comprising an embedded system such as a microprocessor card and the prover entity comprising an embedded card reading system.

ABSTRACT

The invention concerns a method for verifying a signature or an authentication between a prover and a verifier based on an asymmetric cryptographic calculation algorithm.

The prover calculates (1) at least one prevalidation value q, which is a quotient of two cryptographic values a, b by the public modulo n, and transmits this value q to the verifier. The verifier calculates (3) the products a*b and q*n and the difference a*b-q*n in order to perform at least one modular reduction without a division operation.

The invention applies to signature or authentication verification between a proving microcomputer and a verifying microprocessor card.

Fig. 1

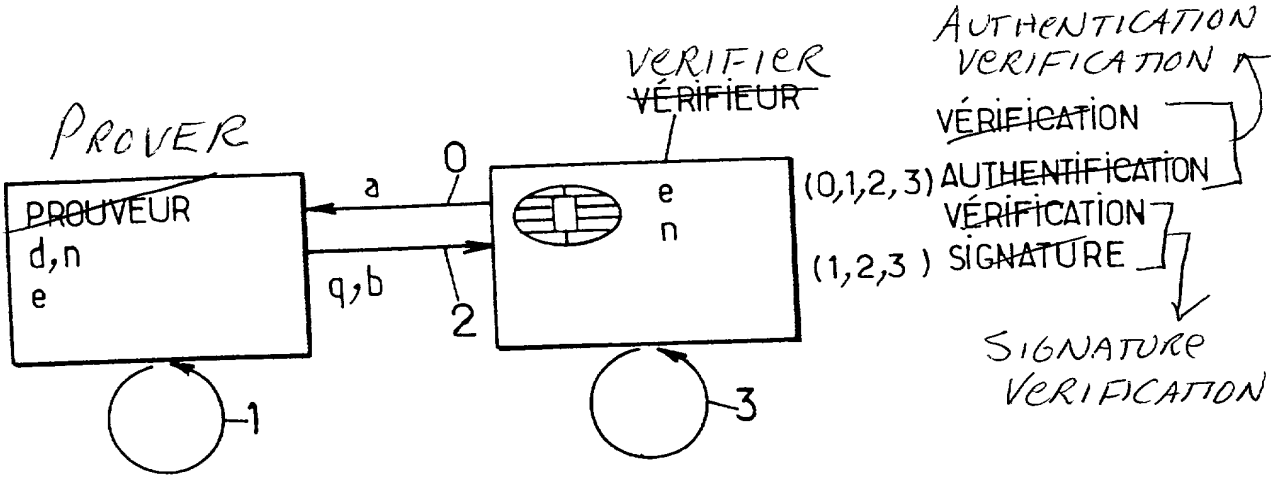


FIG.1.

$q = a * b / n$

$b = \begin{cases} a^d \bmod n & \text{si (0,1,2,3)} \\ s = Sd(M) & \text{si (1,2,3)} \end{cases}$

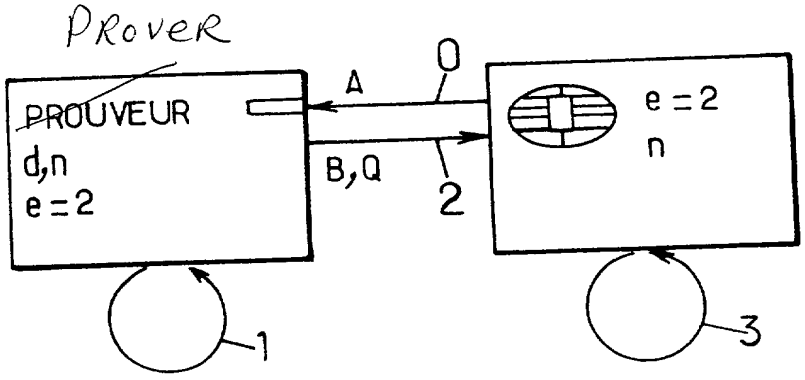
if

if

$a * b$

$q * n$

$a * b - q * n$



$R = B = A^d \bmod n$

$Q = B * B / n$

FIG. 2a.

$D_{AR} = B * B - Q * n$

$D_{AR} = A$

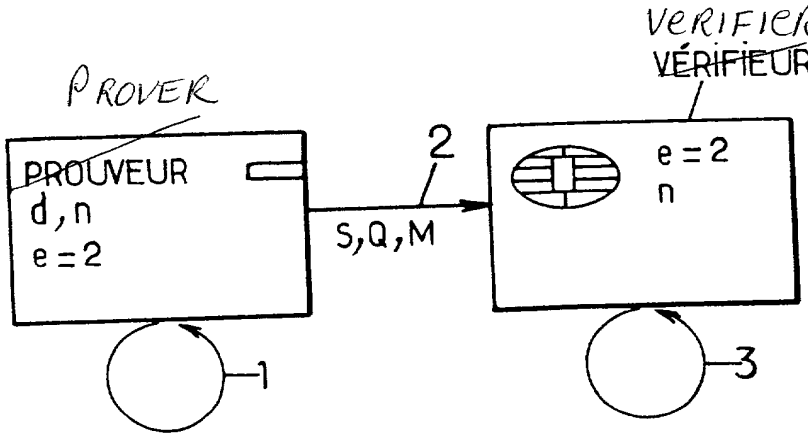
$D_{AR} = n - A$

$D_{AR} = C * A \bmod n \} = C * A$ SI $C * A < n$

$D_{AR} = -C * A \bmod n \} = C * A - n$ SINON

IF

IF NOT



VÉRIFICATION
SIGNATURE SIGNATURE
VERIFICATION

$R = S = Sd(M)$

$Q = S * S / n$

$D_{SR} = S * S - Q * n$

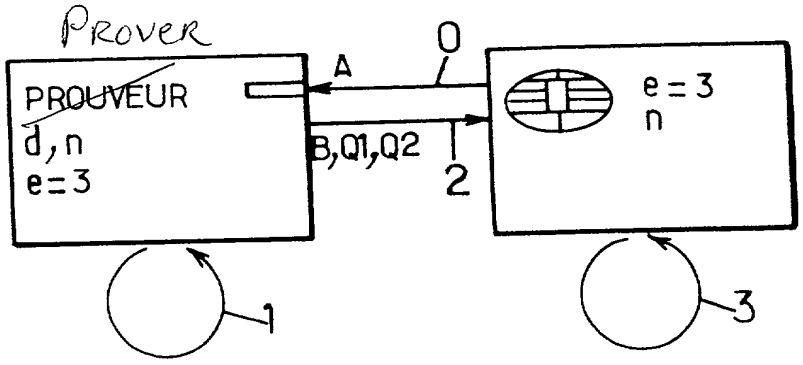
$D_{SR} = f(M)$

$= n - f(M)$

$= C * f(M) \bmod n = C * f(M)$ if $< n$

$= C * f(M) \bmod n = C * f(M)$ SINON IF NOT

FIG.2b.



VÉRIFICATION
D'AUTHENTIFICATION
AUTHENTICATION
VERIFICATION

$R = B = A^d \bmod n$

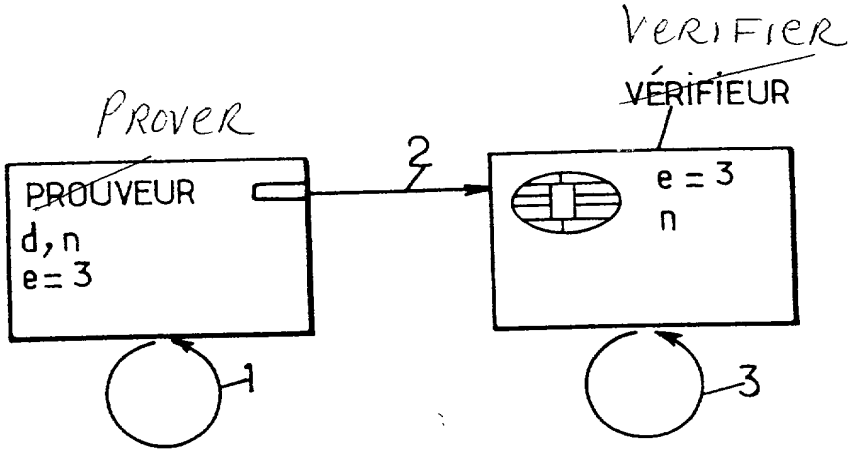
$Q1 = B * B / n$

$Q2 = B(B * B - Q1 * n) / n$

$D_{ARSA} = B(B * B - Q1 * n) - Q2 * n$

$D_{ARSA} = f(A) = A$

FIG.3a.



$R = S = Sd(M)$
$Q1 = S * S / n$
$Q2 = S(S * S - Q1 * n)/n$

$D_{SRSA} = S(S * S - Q1 * n) - Q2 * n$
$D_{SRSA} = f(M)$.

FIG.3b.

Declaration and Power of Attorney For Patent Application
Declaration Pour Demandes de Brevets Avec Pouvoirs

French Language Declaration

En tant qu' inventeur nomme ci-après, Je déclare par le présent acte que:

Mon nom, mon domicile, mon adresse postale, ma nationalité sont ceux qui figurent ci-après,

Je déclare que je crois être l'inventeur original, premier et unique (si un seul nom figure sur le présent acte) ou un des co-inventeurs, originaux et premiers (si plusieurs noms figurent sur le present acte) du sujet revendiqué et pour liquel un brevet est demande sur la base de l'invention intitulée:

Procédé de vérification de signature ou d'authentification.

dont la description
(cocher la case correspondante)

☒ est annexée au présent acte.

☐ a été déposée _____

Numéro de série de la demande _____

et modifiée le _____ (si approprié)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

_____

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on _____ as

Application Serial No. _____

and was amended on _____ (if applicable)

Je déclare par le présent acte avoir examiné et compris le contenu de la description identifiée ci-dessus, revendications y compris, et le cas échéant telle que modifiée par l'amendment cité plus haut.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais le devoir de divulguer l'information qui est en rapport avec l'examen de cette demande selon Titre 37 du Code des Reglements Fédéraux §1.56(a).

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

French Language Declaration

Je revendique par le présent acte le bénéfice de priorité étrangère selon Titre 35, du Code des Etats-Unis, §119 de toute demande de brevet ou d'attestation d'inventeur énumérée ci-après, et j'ai identifié également ci-après toute demande étrangère de brevet ou d'attestation d'inventeur ayant une date de dépôt antérieure à celle de la demande pour laquelle la priorité est revendiquée.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior foreign applications

Demande(s) de brevet antérieure(s) dans un autre pays:

(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	Priority claimed / Droit de priorité revendiqué: Yes Oui	No Non
FR 99 04975	France	20 04 1999	☒	☐
			☐	☐
			☐	☐

Je revendique par le présent acte, le bénéfice selon Titre 35 du Code des Etats-Unis, §120 de toute(s) demande(s) américaines énumérée(s) ci-après et, dans la mesure où le sujet de chacune des revendications de cette demande n'est pas divulgué dans la demande américaine antérieure, de la façon définie par le premier paragraphe de Titre 35 du Code des Etats-Unis, §112, je reconnais le devoir de divulguer l'information pertinente selon Titre 37 du Code des Réglements Fédéraux, §1.56(a), toute information qui se présente entre la date de dépôt de la demande antérieure et la date de dépôt de la demande, soit nationale, soit internationale PCT.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) (No. de Demande)	(Filing Date) (Date de Depôt)	(Etat) (brevetée, pendante, abandonné)	(Status) (patented, pending, abandoned)
PCT/FR00/01047	20/4/2000	PENDING	

Je déclare par le présent acte que toutes mes déclarations, à ma connaissance, sont vraies et que toutes les déclarations faites à partir de renseignements ou de suppositions, sont tenues pour être vraies; de plus, toutes ces declarations ont été faites en sachant que de fausses déclarations volontaires u autres actes de même nature sont sanctionées par une amende ou un emprisonnement, ou les deux, selon la Section 1001, du Titre 18 de Code des Etats-Unis et que de selles déclarations délibérément fausses peuvent compromettre la validité de la demande ou du brevet délivré.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

French Language Declaration

POUVOIR: En tant qu'inventeur, je désigne l'(les) avocat(s) et/ou l'(les) agent(s) suivant(s) pour poursuivre la procédure de cette demande et traiter toute affaire la concernant supris du Bureau des Brevets et de Marques:

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (*list name and registration number*)

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

Adresser toure correspondance à:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Send Correspondence to:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Adresser toute communication téléphonique à: (*Nom*) (*Numéro de téléphone*)

Edward J. Kondracki, Esq.
(703) 998-3302

Direct Telephone Calls to: (*name and telephone number*)

Edward J. Kondracki, Esq.
(703) 998-3302

Nom complet du seul ou premier inventeur	Full name of sole or first inventor
GOUBIN Louis	
Signature de l'inventeur — Date: 28 mai 1999	Inventor's signature — Date
Domicile: 3 rue Brown-Séquard 75015 PARIS FRANCE FRX	Residence
Nationalité: Française	Citizenship
Adresse Postale: 3 rue Brown-Séquard 75015 PARIS FRANCE	Post Office Address
Nom complet du second co-inventeur, le cas echeant	Full name of second joint inventor, if any
PATARIN Jacques	
Signature de l'inventeur — Date: 28 mai 1999	Second Inventor's signature — Date
Domicile: 11, rue Amédée Dailly 78220 VIROFLAY FRANCE FRX	Residence
Nationalite: Française	Citizenship
Adresse Postale: 11, rue Amédée Dailly 78220 VIROFLAY FRANCE	Post Office Address

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)